UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/992,582	11/16/2001	Stephen M. Hitchen	1152-2U	8250

29973   7590   05/07/2007
CAREY, RODRIGUEZ, GREENBERG & PAUL LLP
ATTN: STEVEN M. GREENBERG, ESQ.
950 PENINSULA CORPORATE CIRCLE
SUITE 3020
BOCA RATON, FL 33487

EXAMINER
WASSUM, LUKE S

ART UNIT	PAPER NUMBER
2167	

MAIL DATE	DELIVERY MODE
05/07/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

PTOL-90A (Rev. 04/07)

MAILED

MAY 0 7 2007

Technology Center 2100

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Application Number: 09/992,582
Filing Date: November 16, 2001
Appellant(s): HITCHEN ET AL.

Steven M. Greenberg
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 16 January 2007 appealing from the

Office action mailed 4 April 2006.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the

brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial

proceedings which will directly affect or be directly affected by or have a bearing on the

Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection

contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is

correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

5,724,578	MORINAGA et al.	03-1998
2002/0035697	MCCURDY et al.	03-2002
2002/0178271	GRAHAM et al.	11-2002

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Morinaga et al. (U.S. Patent 5,724,578) in view of **McCurdy et al.** (U.S. Patent

Application Publication 2002/0035697) in view of **Graham et al.** (U.S. Patent Application

Publication 2002/0178271).

These rejections are set forth in a previous Office action, mailed 4 April 2006.

For the convenience of the Honorable Board of Appeals, the rejection of

representative independent claim 1 is reproduced herein.

Regarding claim 1, **Morinaga et al.** teaches a collaborative file rights

management method as claimed, comprising: ·

a) identifying a file input/output (I/O) request to access a file, said file I/O request

originating in an authoring application (see col. 4, lines 20-23, disclosing

that all requests for files are received by the file transaction control unit);

b) automatically extracting digital rights management data appended to said file

(see disclosure of the file control block, col. 4, lines 32-61); and

c) providing said file to said authoring application (see col. 4, lines 32-38; see also

col. 7, lines 35-46).

Morinaga et al. does not explicitly teach a collaborative file rights management

method including the step of managing access to said file in said authoring application

based upon said extracted digital rights management data.

McCurdy et al., however, teaches a collaborative file rights management method

including managing access to said file in said authoring application based upon said

extracted digital rights management data (see paragraphs [0137] through [0140]).

It would have been obvious to one of ordinary skill in the art at the time of the

invention to perform the claimed intercepting, detecting and quashing steps in

cooperation with an authoring application, since digital rights management dictates

that users with no rights to individual parts of a document be prohibited from copying

not only an entire document, but the individual protected parts (see paragraphs [0137]

and [0138]).

Neither **Morinaga et al.** nor **McCurdy et al.** explicitly reaches suppressing said file I/O request.

Graham et al., however, teaches a system which provides selective access and usage management to files available from one or more file systems or sources (see paragraph [0011]) through the use of a filter driver, wherein a request dispatched to the file system is intercepted and suppressed by the filter driver, and wherein the filter driver interfaces with the file system and adds additional functionality beyond that offered by the existing file system (see paragraphs [0140] and [0141]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to intercept and suppress file I/O requests in order to implement usage management, since this allows clients to access and utilize files without changing the process for accessing files in any way from the user's perspective, i.e., users continue to use Network Neighborhood or content management software, and other standard applications to access remote storage drives and directories (see paragraphs [0138] and [0139]).

(10) Response to Argument

This Examiner's Answer will address the Appellants' arguments in the order in which they appear in the appeal brief.

A. Issue 1

<u>Claims 1-20 are properly rejected under 35 U.S.C. § 103(a) as being unpatentable over Morinaga et al. (U.S. Patent 5,724,578) in view of McCurdy et al. (U.S. Patent Application Publication 2002/0035697) in view of Graham et al. (U.S. Patent Application Publication 2002/0178271).</u>

Regarding claims 1-20, the Appellants argue that **(1) Graham's** interception and modification of a file system request is not the same as the claimed suppression of a file I/O request, that **(2) Graham's** proxy system bears no relation to **Graham's** filter driver, and that **(3) Graham** cannot be reasonably combined with **Morinaga** as **Graham** teaches the mere modification and forwarding of a file I/O request rather than a suppression of a file I/O request.

In response, the examiner presents the following arguments.

Regarding argument **(1)** [that **Graham's** interception and modification of a file

system request is not the same as the claimed suppression of a file I/O request], the

examiner respectfully disagrees.

The Appellants' independent claims include the limitation that a user's I/O

request to access a file is 'suppressed'.

The Appellants' specification discloses that a file security filter driver resides in

the system kernel to monitor kernel-level file I/O requests, and that when an I/O request

is detected, the requested file is examined to determine whether the file can be

processed by the file access management system (paragraph [0037]).

If so, the I/O request is quashed, the requested file is retrieved, digital rights

management data is extracted therefrom and examined for access policy and digital

rights associated with the file, and a determination is made as to whether access to the

file shall be permitted (paragraph [0038]).

If access is not granted, a message can be posted to the application to notify the

user that the access policy associated with the requested file does not permit access by

the user (paragraph [0038]). If access is granted, the file is provided to the authoring

application which manages access to the file based upon the extracted digital rights

management data (paragraph [0041]).

Based upon these disclosures, it can be concluded that the claimed 'suppression'

of the I/O command means that the command issued by the user application is

intercepted by the filter driver, which then issues its own request to access the file in

order to inspect the digital rights management data associated with the file to determine

whether the requesting user should be permitted access to the file.

The rejection of record is based upon a combination of three references,

Morinaga et al., McCurdy et al. and **Graham et al.**

All three of these references are concerned with providing users with access to

content, while limiting the user's access based upon digital rights management data

associated with the content.

The **Morinaga et al.** reference teaches a system for managing access to files based

upon access rights associated with the files.

In particular, **Morinaga et al.** teaches

"The file server 10 comprises a control unit 12 and a file
storing unit 14 as shown in FIG. 1." (col. 4, lines 1-2).

"The control unit 12 comprises a transaction control unit 121
and a file operation control unit 122. The file transaction control
unit 121 receives all requests for operating files input by users who
logged in through the end terminal units 21(1), 21(2),..., 21(n)."
(col. 4, lines 20-24).

These disclosures anticipate the claimed "identifying a file input/output request

to access a file, said file I/O request originating in an authoring application" limitation.

"The file operation control unit 122 comprises a central
control unit 123, an access right control unit 124, a link data control
unit 125 and a file data control unit 126. The central control unit
123 selectively controls the access right control unit 124, the link
data control unit 124 and the file data control unit 126 in
accordance with the contents of each request. The access right
control unit 124 checks the access right on the file and the link
provided to each user, and changes the status of the access right if
necessary." (col. 4, lines 30-38).

"FIG. 3A shows a structure of the file control block. The file
control block stores information for managing a file such as a file
access right of each user, a file name and a file creator. A file access
right is a right which is given to and executed by each user for
operating a file. The file access right consists of a visible right, a
reading right, a writing right, a copying right, a deleting right and
an owner right." (col. 4, lines 45-52).

These disclosures anticipate the claimed "automatically extracting digital rights

management data appended to said file" limitation.

> "When another user who logged in through the end terminal
> unit 21(2) access a file stored in the file server 10 which file was
> produced in accordance with the above-mentioned procedure, the
> access right control unit 124 determines whether the access to file
> can be accepted by referring to the access rights set in the file
> control block of the file. If the access is acceptable, the file data
> control unit 124 [sic] reads data of the file, and the data is
> transferred from the file server 10 to the end terminal unit 21(2) via
> the network unit 50. The user then works on the file at the end
> terminal unit 21(2) in accordance with the corresponding access
> right." (col. 7, lines 35-46).

This disclosure anticipates the claimed "providing said file to said authoring

application" limitation.

While the **Morinaga et al.** reference discloses at col. 7, lines 44-46, that the user

works on the file in accordance with the corresponding access right, the **McCurdy et al.**

reference more explicitly discloses the claimed limitation of "managing access to said

file in said authoring application based upon said extracted digital rights management

data" in paragraphs [0137] and [0138]:

"Once the content is secured, the various elements in the file
are managed based on simple rights associated with each element
in the file. Table 3 shows representative example of rights and
elements contemplated in accordance with an embodiment of the
invention.

Referring to Table 3, if the rights (e.g., print and/or tear) are
not granted for a particular magazine element, that functionality is
disabled for the particular magazine element. For example, a given
set of rights for a given magazine may give user the right to print
advertising, but not pictures or graphics. Those skilled in the art
will recognize that rights other than printing and tearing (e.g.,
saving as a separate document, "cut and paste" type copying of
portions of the magazine into another electronic document,
modification of content), and the like, may or may not be spelled
out for a given magazine."

Neither the **Morinaga et al.** nor the **McCurdy et al.** reference explicitly teaches

the claimed "suppressing" feature.

The **Graham et al.** reference discloses a system for managing distributed file

access through the use of a filter driver.

Graham et al. discloses that

"The file system driver manages all communications with
the client 150 and proxy system 110...In the case of the client
module 230 filter driver, rights and encryption management and

the proxy file management system secure transport protocol is
implemented." (paragraph [0140]).

Thus **Graham et al.** discloses that rights management is implemented as a filter

driver that is part of the client module 230, which manages the client system's access to

files on content source 160 via the proxy server 110.

Graham et al. also discusses broadly how the filter driver manages access to files

in accordance with rights management:

> "This filter driver allows the client module 230 to intercept
> and modify file requests to and from file servers as required."
> (paragraph [0141]).

This functionality, however, is also discussed earlier in the specification:

> "In the preferred embodiment, the client module 230
> evaluates the usage policy inside the kernel of the client's OS."
> (paragraph [0117]).

> "The usage rights are enforced through the trapping of
> kernel-level OS calls that are tied to a process list...The client
> module 230 is between the application and operating system,
> which allows the client module 230 to understand what the

application requests from the OS, and modify these requests as needed to control how information is used. (paragraph [0118]).

"When a call is made to the client's OS that has been identified as potential source of data movement, the client module 230 intercepts the call between the application and the OS...if it is determined that the call will result in a protected file being acted on, then the usage rights of that particular file are evaluated from within the kernel. If the call is within the allowed functionality set forth in the usage policy, then it is allowed. If the call is not allowed, then the call is blocked and the user is notified." (paragraph [0119]).

"The client module 230 is designed to be the final line of defense against unauthorized use of enterprise information. Its focus is on the enforcement of usage policy applied by the proxy system 110, and the highly specific auditing functionality." (paragraph [0122]).

"Client module 230 enforces usage policies at each user host [and] provides the following services:
5) Enforcement Mechanisms 442 - As part of the content service module 234, usage policies are enforced by the redirection of operating system calls to proxy file management system defined enforcement software. Redirected system calls will be performed where access is consistent with received usage policies." (paragraphs [0126] and [0131]).

These passages make clear the fact that the filter driver, which "allows the client module 230 to intercept and modify file requests to and from file servers as required" (paragraph [0141]) includes the claimed "suppressing" feature.

Requests for file access dispatched to the OS are intercepted and redirected to

proxy file management system defined enforcement software (paragraph [0131]), which

means that the original I/O request (as dispatched from a client application) has been

suppressed, since said I/O request has been prevented from reaching the OS module to

which it had been directed.

The enforcement software then handles the I/O request in accordance with the

usage policies of the requested file. Clearly, at a minimum, **Graham et al.** discloses a

system wherein a file I/O request dispatched from an application has been suppressed

in the instance where the request has been blocked (paragraph [0119]).

Even in the case where the request is modified to control how information is

used (paragraph [0118]), the modified request is dispatched from the enforcement

software, meaning that the original I/O request issued from the client application has

been suppressed.

The operation undertaken by the filter driver of the client module in **Graham et**

al. is analogous to that disclosed by the Appellants' invention, in that a request

dispatched to the OS for access to a file is intercepted, the usage policies associated with

the requesting user and the requested file are considered, and the file is then provided

to the requesting application consistent with the usage policies of the requested file.

Regarding argument **(2)** [that **Graham's** proxy system bears no relation to

Graham's filter driver], the examiner respectfully disagrees.

Paragraphs [0021] and [0022] discuss a proxy system. In paragraph [0020],

Graham et al. discloses that "A proxy system (including a set of one or more proxy

servers) is disposed between one or more client devices and at least one content

source.", which means that the proxy *system* encompasses more then merely the proxy

servers.

As discussed above, **Graham et al.** discloses a filter driver that is part of the

client module 230, which manages the client system's access to files on content source

160 via the proxy server 110 (paragraph [0140]). Also taught at paragraph [0123] is the

following:

> "In the preferred embodiment, client module 230 enforces
> authorization and access control policies by redirecting OS
> primitives, as previously described. Hence, on each client device
> 150 a set of proxy file management system 100 libraries is installed."

Also, as previously discussed, the client module 230 enforces usage policies at

each user host [and] provides an Enforcement Mechanism service that enforces usage

policies by redirecting operating system calls to proxy file management system defined

enforcement software. (paragraphs [0126] and [0131]).

Clearly, the filter driver, which allows the client module 230 to intercept and

modify file requests to and from file servers as required (paragraph [0141]) is part of the

proxy system (as that term is used in paragraphs [0021] and [0022]), and the teachings

regarding the interception of I/O requests in paragraphs [0140] and [0141] are analogous

to the disclosures of paragraph [0022] that

> "...when an end-user requests a file, the proxy system
> obtains verification of the authentication of the user from the
> authentication system and in cooperation with the policy system,
> the proxy system determines if the requesting user has the right to
> access the file. If access is granted, the proxy system provides the
> file, in a secure and encrypted manner, with additional information
> (e.g., usage rights and encryption/decryption keys) to the end-user
> client device."

Regarding argument (3) [that **Graham** cannot be reasonably combined with

Morinaga as **Graham** teaches the mere modification and forwarding of a file I/O

request rather than a suppression of a file I/O request], the examiner respectfully

disagrees.

As discussed above with regard to argument **(1)**, the **Morinaga et al.** reference

discloses a file transaction control unit 121 that receives all requests for operating files

input by users who logged in through the end terminal units 21(1), 21(2),..., 21(n)." (col.

4, lines 20-24).

The **Graham et al.** reference is relied upon in the rejection of record for its

explicit disclosure of the suppression of the file I/O request. As discussed above with

regard to arguments **(1)** and **(2)**, the **Graham et al.** reference discloses the claimed

suppression step, contrary to the 'mere modification and forwarding' of a file I/O

request, as alleged by the Appellants.

The examiner has provided a proper motivation for incorporating the

'suppressing' feature disclosed by the **Graham et al.** reference into the collaborative file

rights management system disclosed by the **Graham et al.** and **McCurdy et al.**

references, as is stated in the rejections of record.

For these reasons, the examiner maintains that the rejections of claims 1-20 are

proper, and should be sustained.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the

Related Appeals and Interferences section of this examiner's answer.

Conclusion

Claims 1-20 are properly rejected under 35 U.S.C. § 103(a).

In light of the foregoing arguments, the Examiner respectfully requests the

Honorable Board of Appeals to sustain the rejections.

For the above reasons, it is believed that the rejections should be sustained.
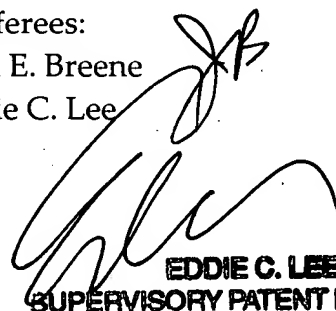
Respectfully submitted,

Luke S. Wassum
Primary Examiner
Art Unit 2167

Conferees:
John E. Breene
Eddie C. Lee

EDDIE C. LEE
SUPERVISORY PATENT EXAMINER

lsw
26 April 2007